Internet Crime Prevention

The Internet places a vast amount of information and exciting experiences at your command. With the click of a computer mouse, the Internet allows you to buy an airline ticket, book a hotel, send flowers to a friend or purchase your favorite stock. However, as the legitimate use of the Internet increases throughout our nation and the world, the wrongful use of the Internet to commit crime and victimize people also increases. The following Internet crime prevention information is meant to help you protect yourself, your loved ones, your friends, your neighbors and your community, and to make your journey on the Internet as safe, secure and crime-free as possible.

COMMON INTERNET CRIMES

Child Exploitation

Children can be sexually exploited, kidnapped, molested and solicited by individuals using online services. One reason is the anonymous nature of the Internet. Another reason is the large number of people using the Internet. Pedophiles contact children on the

Internet through E-mail messages, electronic bulletin boards and public chat rooms. Pedophiles will make telephone contact with victims by having children call collect. The pedophile's telephone number will not appear on their parent's telephone bill. Pedophiles also will purchase a prepaid telephone card and give potential child victim's a toll-free access number enabling children to call from anywhere they choose.

Pedophiles often will convince children to send them a photograph. Pedophiles will offer children money for their photographs and/or pose as professional photographers to obtain nude, graphic or sexually explicit photographs of children. Pedophiles commonly attempt to lower the inhibitions of children through deception, in an attempt to lead children into other sexual conversations or acts. There are a number of ways adults can protect children from becoming victims of pedophiles on the Internet.

The following are some examples:

- Choose an online service that offers parental control features.
- Purchase blocking software and design your own safety system.

- Monitor children that are online and monitor the time they spend online.
- Ensure that children never reveal identifying information about themselves on the Internet in a public chat room, on an electronic bulletin board or in their E-mail messages.
- Ensure that children do not give out personal information about themselves, such as their age.
- Consider using a pseudonym or unlisting your child's name;
- Get to know the services your child uses.
- Block out objectionable material through your Internet service provider.
- Never allow a child to arrange a face-to-face meeting with another computer user without permission from a parent or guardian.
- Ensure that children never respond to messages or bulletin board items that are suggestive, obscene, belligerent or threatening.
- Encourage children to tell you whenever they encounter such messages;
- If you or your children receive a message that is harassing, sexual in nature, or threatening,

- forward a copy of the message to your service provider and ask for assistance.
- If you become aware of the transmission, use, or viewing of child pornography while online, report it to the National Center for Missing and Exploited Children.
- Teach children that people online may not be who they seem or say.
- Teach children online service providers never ask for passwords, so they should never give their password to anyone.
- Teach children that everything they read or see on the Internet may not be true.
- Teach children to never let anyone pressure them into doing something they feel uncomfortable doing.
- Teach children to never enter an area on the Internet that charges for services without first asking permission from a responsible adult.
- Some children have access to the Internet at school. Check with the school authorities to ensure that your children are properly supervised and monitored by a responsible adult.
- Know children's friends and their parents.

Fraud

Internet fraud takes many forms. The Internet's promise of substantial consumer benefits is coupled with the potential for fraud and deception. Fraud operators are opportunists who are among the first to appreciate the potential of a new technology. There is nothing new about Internet fraud. However, the size and potential market, relative ease, low cost and speed with which a scam can be perpetrated has increased tremendously.

Unsolicited Commercial E-Mail

Internet service providers report handling 60 million electronic messages per day. Estimates of Unsolicited Commercial E-mail (UCE) indicate it comprises as much as one-third of the total E-mail traffic. This ever-increasing volume of UCE strains the capacity of online service providers and threatens the development of the Internet as a conduit for commerce. Beyond the sheer volume and potential annoyance of UCE, many UCE messages also may be misleading or deceptive.

Teaser Pages

The Internet is full of fraudulent schemes. Some web pages "tease" individuals with promises of easy money for little or nothing. These scams include phony scholarships, travel programs, weight loss programs

and others.

High Pressure Sales

A high-pressure sales pitch may sound exciting. However, as a rule, such a pitch should be resisted. Before you invest any money, take your time. Get a second opinion from a financial planner, an attorney or an accountant you can trust. Finally, research the company's reputation. Call your local consumer protection agency in the city where the company is headquartered for more information.

Following are come-ons frequently used by scam artists:

- "We don't make money unless you make money."
- "I know you get offers everyday from people who tell you they're going to make you rich. I can make it easy for you to make your decision based on actual facts."
- "This opportunity is the best chance to make extra money for guys who work for a living; guys like you and me."
- "I've been in this business for 20 years and I can tell you this; I know of no other program that is legal, easy to afford and can bring in this kind of big money from such a small investment."
- "I know this can work for you and I personally guarantee your success, right down to the last penny."
- "Give me one percent of your trust

- and I'll earn the other 99 percent when you see the return."
- "Of course there is a risk, there is a risk in everything."
- "Sure we could finance this venture ourselves, however, we're trying to build a power base for the future for folks like you."
- "We're talking about a cash cow here, it's going fast and I need your check tomorrow at the latest."
- "I can't be lying, there are laws against lying."

The Risk-Free Scam

Many times this scam solicits its victims with exotic-sounding investments such as wireless cable projects, prime bank securities or fictitious business ventures overseas. Promoters misrepresent risk to "investors" by comparing their offer to something safe, such as bank security Pyramid schemes are similar to multideposits. Many times the investment offer never really exists.

The Pump and Dump

This is a stock scam. Messages are posted on the Internet urging readers quickly to buy stock that is poised for rapid growth. The message writer about an impending development. The reality is that the writer stands to gain by selling or buying stock shares after the price goes up or down.

This ploy is normally used with

unregistered, little known and thinly traded stocks.

The Hijack

The Hijack is a relatively new form of fraud unique to the Internet. Consumers are prompted to download a purported "viewer program" to see computer images for free. Once downloaded, the consumer's computer is "hijacked" by the viewer program which turns off the consumer's modem speakers, disconnects the computer from the local Internet provider, dials an international number and connects the consumer to a remote site. The expensive international costs are charged to the consumer's telephone bill until the telephone is turned off.

Pyramid Schemes

level marketing. Pyramid schemes provide financial incentives to recruit new distributors. They are generally prohibited because it is a mathematical certainty that the pyramids will collapse when no new distributors can be recruited. When that happens, most people lose their money. The Internet offers a fast lane for pyramid builders often claims to have inside information by facilitating a large-scale recruitment pool in little or no time. Be extremely cautious if a promoter offers you an extremely large short-term return on any investment, particularly if there is a disclaimer that the investment is

"high-risk and you could lose all of your money." Additionally, if there are no written claims delineating the returns on other's investments, you are quite possibly looking at a pyramid scheme. Beware of all get-rich-quick schemes. If a deal seems too good to be true, it probably is.

Gambling

One of the greatest potential dangers for fraudulent loss posed for people using the Internet is gambling. There are as many as 200 gambling sites on the Internet. Consumers may gamble on sports, Blackjack, Keno, Roulette, etc. Gambling on the Internet is especially risky because gambling is an unregulated industry and currently, there is no effective way to control it. Companies based in foreign countries using foreign bank accounts are able to easily bilk consumers out of their money. Many times Internet "gamblers" are unable to contact the companies with whom they placed their bets to collect their winnings. Gambling on the Internet exposes consumers to fraud, civil liability and possible criminal liability.

Online Auctions

Online auctions are popular to many people who use the Internet. Generally, online auctions are person-to-person sales where individuals bid for various types of merchandise. The highest bidder then pays in advance of receiving the merchandise. A growing problem is sellers failing to deliver purchased merchandise that consumers have purchased.